SMALL WARS JOURNAL

smallwarsjournal.com

A Reserve Component Initiative to Defend DoD and National Cyberspace[1]

by David M. Hollis

Background

The United States is under increasing threat from both nation state and non-nation state cyberspace domain aggressors. An effective attack against vulnerable elements of our critical infrastructure could produce major and lasting damage to our national economy, military capability, and our cultural way of life. The ability to conduct Cyberspace domain operations is a predicate to both successful military operations and successful private sector operations such as in the economic/financial, health, telecommunications, logistics, and energy operations sectors. Therefore, dominating this domain is critical to a functioning economy, national security, and to ensuring success in the other warfighting domains (air, sea, land, and space). Identifying, defending, and (potentially) reconstituting cyberspace key terrain is an essential task for dominating this domain.

The military (DoD and the Service‘s) approach to defending the cyberspace domain, while considerably better than any other US government (USG) entity: is still fragmented, unorganized, and not under effective command and control (C2)[2]; requires integrated individual and collective training; and lacks effective inter-agency national policy to achieve full effectiveness. The establishment of US Cyberspace Command (USCYBERCOM) is a very effective start toward resolving many of these shortfalls. [3] Another shortfall: the extensive

[1] This article incorporates some of the concepts originally contained in the visionary ―White Paper Proposal: Rapidly Harness America‘s Reserve Cyber Human Capital in a Dynamic Organizational Construct to Defend our Nation‘s Critical Infrastructure from Cyber Attack” an unclassified undated white paper by MG David Lacquement, J3 USCYBERCOM, and further developed in multiple conversations with Brig Gen Tom Thomas, USCYBERCOM Guard/Reserve Advisor; Guy M. Walsh, J-3 Strategic Initiatives, USCYBERCOM; CDR Ron Gorman, GRMO, USCYBERCOM; and CAPT Marcia Flatau Joint Cyber Reserve Unit (JCRU) and USNR Element Commander, USCYBERCOM. Much credit for this article belongs to these five highly-accomplished professionals; on the other hand, any poor grammar, bad ideas, and bone-headed mistakes belong entirely to me.

[2] GAO ―Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities” GAO-11-421 ―Consequently, the services are moving forward using disparate, service-specific approaches to operationalizing cyberspace without knowing exactly what mission requirements they will be required to meet for U.S. Cyber Command. For example, Navy and Air Force officials told us that they are leveraging reserve component resources and taking personnel from existing career fields to avoid having to increase service end strength. Further, the two services are taking very different approaches to rearranging their career fields to varying degrees in order to further improve their efforts to recruit and retain cyber personnel, and they are doing this in different ways as they define new service-level personnel needs, maintain old ones, anticipate future U.S. Cyber Command personnel needs, and attempt to recruit, retain, and train for all three needs. Army, Navy, and Marine Corps officials told us that they are largely rearranging existing specialty codes in communications and cryptologic fields and giving their personnel new tasks and some new training, while the Air Force has created entirely new career specialties for cyberspace operations.”

[3] GAO, ―Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities,”
GAO-11-75 July 25, 2011 ―DOD's organization to address cybersecurity threats is decentralized and spread across various offices, commands, military services, and military agencies. DOD cybersecurity roles and responsibilities are vast and include developing joint policy and guidance and operational functions to protect and defend its computer networks. DOD is taking proactive measures to better address cybersecurity threats, such as developing new organizational structures, led by the

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **10 NOV 2011**	2. REPORT TYPE	3. DATES COVERED **00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE
A Reserve Component Initiative to Defend DoD and National Cyberspace

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Office of the Undersecretary of Defense for Intelligence?s (USD(I)) Cyberspace, ,Warfighter Integration, and Strategic Engagement Division (CWISE),Washington,DC,20301-1400

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**12**	

capabilities of the military‘s Reserve Components are not effectively utilized to conduct and support cyberspace domain operations. For example, other major military powers use their reserve component forces to support full-spectrum military and national operations in cyberspace domain.[4] (see Figure 1) In response, there are several initiatives to utilized DoD‘s RC forces to support national cyberspace objectives.[5] So while we have considerable cyberspace capability in both the Active and Reserve Components, much of it is unorganized, fragmented, the training is non-existent or uneven, and cyberspace domain oriented C2 is primitive if not non-existent.

Proposed Solution

One initiative that could be utilized to defend the nation, mitigate serious threats, and provide cyberspace domain units for theater warfighting/overseas deployment is a synchronized national approach leveraging the Defense Department‘s Reserve Component (RC) forces to secure the country‘s critical infrastructure from growing cyber threats. Thousands of military Reservists, many of whom have professional civilian careers in Information Technology (IT),

establishment of the U.S. Cyber Command, to facilitate the integration of cyberspace operations. However, it is too early to tell if these changes will help DOD better address cybersecurity threats. …DOD has assigned authorities and responsibilities for implementing cyberspace operations among combatant commands, military services, and defense agencies; however, the supporting relationships necessary to achieve command and control of cyberspace operations remain unclear. In response to a major computer infection…Without complete and clearly articulated guidance on command and control responsibilities that is well communicated and practiced with key stakeholders, DOD will have difficulty in achieving command and control of its cyber forces globally and in building unity of effort for carrying out cyberspace operations. DOD has identified some cyberspace capability gaps, but it has not completed a comprehensive, departmentwide assessment of needed resources, capability gaps, and an implementation plan to address any gaps. For example, U.S. Strategic Command has identified that DOD's cyber workforce is undersized and unprepared to meet the current threat, which is projected to increase significantly over time.”

[4] For an example of foreign military use of reservists in conducting cyberspace operations, see John A. Nagl and Travis Sharp ―Operational for What? The Future of the Guard and Reserves” Joint Forces Quarterly Vol 59 ―In recent years, the PLA has increasingly recruited civilian reservists who lack prior military service but possess high-tech skills with military applicability. For example, reservists employed in the chemical industry serve in chemical warfare units, and reservist telecommunications workers have been assigned to new PLA units specializing in information warfare and information operations. These highly skilled reservists play a growing role in China's evolving antiaccess/ area-denial strategy of using sophisticated cyber and electronic attacks to degrade the U.S. military's battle networks, forward bases, and maritime forces and thereby inhibit U.S. power projection capabilities. Another example is Laura L. Knapp, MAJ, USA ―Interpreting Chinese Cyber Attacks of 2007: Indicators of China‘s Cyber Warfare Strategy” Air Command and Staff College (April 2008), found at: https://www.afresearch.org/skins/rims/display.aspx?moduleid=be0e99f3-fc56-4ccb-8dfe-670c0822a153&mode=user&action=downloadpaper&objectid=c6996c76-8f78-4da2-bffe-e84bc805a494&rs=PublishedSearch ―With a population base of 1.3 billion and rising, China has tremendous resources to implement a cyber campaign plan. In a very primitive operation, China could utilize citizens‘ computers to host a botnet and conduct a simple distributed denial of service attack, which is what Russian hackers executed against Estonia. A more comprehensive interpretation of People‘s War involves using civilian hackers, the information technology industry, the cyber security forces, and the PLA reserve cyber forces to assist the PLA in conducting sophisticated cyber operations implementing the strategies of China‘s military tradition….Several of the Chinese military authors describe the requirement for cyber warfare units in the active-duty PLA organization; additionally, the same authors call for regionally aligned reserve (or militia) units that also conduct cyber operations….The PLA‘s formation of cyber reserve, or militia, forces is even more significant. The 2006 Department of Defense Report on the PLA assessed, ―During a military contingency, [militia or reserve] information warfare units could support active PLA forces by conducting ‗hacker attacks‘ and network intrusions, or other forms of cyber warfare, on an adversary‘s military and commercial computer systems, while helping to defend Chinese networks.” Several cyber reserve forces already exist in the cities of Datong, Siamen, Shaghai, Echeng, and Xian, as well as the Shenyang and Guangzhou provinces. These forces recruit members from colleges and universities and the information technology industry. The PLA Daily reported, ”We have created a reserve telecom force structure with a reserve telecom regiment as the backbone, with an information industrial department as the base…have built a reserve contingent…with highly qualified computer experts, network monitoring experts.””

[5] Initiatives such as ―DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE,” 14 July 2011, Page 11 ―Paradigm-shifting approaches such as the development of Reserve and National Guard cyber capabilities can build greater capacity, expertise, and flexibility across DoD, federal, state, and private sector activities”

cyberspace operations, and in related fields, could rapidly be organized in a focused Joint RC Command, subordinated to USCYBERCOM, and responsive to national homeland security. This command (the Joint Reserve Cyberspace Command or JRCC, see figure 2) could be organized both regionally and by IT functional area, and be rapidly employed to increase the security of America‗s most critical cyberspace domain infrastructure in both the government and private sectors. USCYBERCOM and the JRCC would provide command and control (C2) of Joint Reserve Cyberspace Brigades (JRCBs) with geographic and/or functional areas of responsibilities (AOR). The rationale for the JRCC would be to:

- Organize RC cyberspace capabilities (individuals, units, equipment, facilities) into defined organizations with clear command and control (C2) architectures (currently much of the cyberspace capabilities of the military Reserve Components are fragmented, unorganized, and not under an effectively C2).
- Concentrate unorganized, low density, high demand (limited and valuable) cyberspace capability into organized units for purposes of Mass (applying and focusing limited resources toward high priorities), Unity of Command, and Economy of Force (logical prioritization of resources) purposes.[6]
- Network the newly created Joint Reserve Cyberspace Brigades (JRCBs) with other Service-specific RC and National Guard cyberspace-capable units for planning, synchronization, and (in some cases) C2 purposes.
- Identify and organize RC personnel with civilian acquired skills (CAS), identify training requirements and gaps, and provide the additional training to bring these professionals to certified standards. The US military currently has difficulty identifying, prioritizing, and employing CAS in its RC personnel inventory.
- Prepare these units though individual and collective training, and conduct demanding exercises that would challenge their capabilities across a separate free-play network domain training/testing range – these units would exercise and conduct fire and maneuver operations within the cyberspace domain with a full-spectrum mission set.

These units, distributed across the United States and networked into a military and government community of cyberspace capable organizations, would conduct the following mission sets:

- Conduct cyberspace security inspections of critical infrastructure and provide recommendations to enhance the security of America‗s critical cyber infrastructure supporting finance, power, health, logistics, communications, and other critical communities.
- Assist government and private sector IT professionals in America‗s critical infrastructure in mediating/repairing major cyber vulnerabilities.
- Conduct missions to increase resilience of critical infrastructure, repairing and mitigating the damage caused by cyberspace domain attack, and assisting in cyberspace domain and power recovery operations after man-made or natural disaster.

[6] For more information on the limited number of, and competition for cyberspace security professionals, see LTC David Hollis and Katherine Hollis, ―Cyber defense: U.S. cybersecurity must-do's" Armed Forces Journal (Feb 2011) found at: http://www.armedforcesjournal.com/2011/02/5432066

- Respond to major cyber incidents and large scale disasters affecting the nation or a specific region with mobile tailored teams of cyberspace professionals, many of whom would have a TS-SCI level understanding of the cyber threat environment
- Maintain skills sets to support full-spectrum cyberspace domain operations
- Provide technical support/advice to state, regional, and local governments to include Title 32 cyberspace operations support capability to law enforcement activities.
- Provide a ready and available pool of cyberspace domain tactical and operational units to support Combatant Commands theater strategy, either by mobilization and deployment overseas into theater or provide reach-back support from bases in CONUS.
- Be prepared to mobilize to conduct military operations in the cyberspace domain and for deployment overseas to support COCOM theater-level and joint task force (JTF) military operations. Also be prepared to mobilize selected key individuals to support USCYBERCOM or COCOM headquarters functions at various levels.

Concept

The SECDEF would direct the military Services to conduct an inventory of their respective RC cyberspace professionals (regardless of Service, branch, or MOS) to include identification of civilian acquired skills. This would need to be followed up with a database mechanism to track and develop identified RC cyberspace professionals, at the USCYBERCOM, Service, and JRCC levels. In conjunction with NORTHCOM, DHS, NGB, and State governments; USCYBERCOM, and the JRCC would then identify the most critical national infrastructure to be protected and assign missions to the geographic and functional JRCBs. The JRCC would have a traditional headquarters staff based approximately on a geographic combatant command (GCC) model with modifications for mission, domain, and location. The JRCBs themselves would be created and geographically based on the Standard Federal Regions (each JRCB would be aligned with other Federal agencies such as FEMA Regions and USAR's Regional Readiness Commands, see Figure 3).[7] BDE HQs would be located in military bases inside their respective Region with subordinate battalions, companies, and detachments located in Joint Reserve Intelligence Reserve Centers (JRICs), active and reserve military installations,

[7] Organizing and deploying RC elements in a geographic fashion to support military and homeland security operational requirements is a common theme with a long history of concept development and employment. For example, at: http://www.globalsecurity.org/military/agency/army/usarc.htm ―The USAR provides regional support, planning, training and response teams tied to the federal requirements for crisis and consequence management against weapons of mass destruction thus leveraging our military and civilian skills." For an example of a geographically distributed RC cyberspace operations organization, see the Army Reserve Information Operations Command (ARIOC) web site at: http://www.usar.army.mil/arweb/organization/commandstructure/USARC/OPS/USARJSTSC/Commands/ARIOC/Pages/default.aspx . The ARIOC has five major subordinate commands with numerous detachment commands located across the US. Also see Maryann Lawlor ―Cyberspace Forces Gear Up" Signal Magazine, (August 2001) for an article ten years ago concerning use of geographically distributed RC forces in cyberspace operations: ―Calling out the reserves to help fight cyberspace battles was the brainchild of the Reserve Component Employment 2005 study released in 1999. Creating virtual organizations that are dispersed throughout the United States to support the information assurance operations of various commands offers several benefits. It addresses concerns about the number of active duty personnel who are leaving military service for more lucrative jobs in the private sector, which could threaten the strength of U.S. information security forces. In addition, the opportunity to satisfy Reserve commitments while remaining near home is appealing to information security experts. As an added perk, many of these reservists work with the latest technology in their civilian jobs, so they bring their proficiency to the front lines of military cyberdefense (SIGNAL, March 2000, page 27). Five joint Reserve virtual information organizations (JRVIOs) currently are being assembled to support the Defense Department‘s five key information operations agencies and joint commands in fiscal years 2001 and 2002."

and various RC armories. The command would be staffed primarily with RC personnel from all the Services with representation from the National Guard.

These JRCBs would include but not be limited to communications/signal, network defense, information operations, cyberspace operations, electronic warfare, network warfare, power generation, and cyberspace intelligence support battalions. These JRCBs would be staffed with cyberspace professionals, many of them cleared to TS-SCI/poly level to provide them access to critical intelligence to enable cyberspace operations. The JRCC and JCRBs would have a skeletal core of full-time AGR/active duty, government civilian personnel, and contractor support for both administrative and technical expertise, and continuity of operations. These units would be further staffed with a layer of traditional RC personnel on 6 month to two year active duty tours with another ‗outer layer' of drilling traditional reservists (SELRES or M-day personnel) who drill one weekend a month and two weeks out of the year. Although these drilling personnel are often viewed as the ‗least productive' on a daily basis, they represent the elemental core of the JRCC – they are the contingency expansion capability, the fundamental reason for the existence of the JRCC.

The JRCC would establish operational relationships and liaisons with respective state National Guard Cyber defense units (Title 32 units) and provide training and technical assistance as needed/requested. The JRCC would coordinate/synchronize across these units on a daily basis. They would also provide C2 across their respective state National Guard Title 32 units upon federalization. There is a clear ‗lanes in the road' between the JRCC /JRCBs and the National Guard cyberspace domain units – the JRCC operates at a national, Title 10 level, JCRBs operate at a regional, Title 10 level, and the National Guard units operate at a state, Title 32 level (unless federalized, in which case they would operate under JRCC's C2 and authority).

Each JRCB controls communications/signal battalions, cyberspace operations (full spectrum cyberspace BNs with offensive cyberwar capabilities in addition to defensive capabilities), information operations, network warfare, intelligence, power generation, electronic warfare, and Network Defense (cyberdefense only) battalions. All brigades and battalions need to contain a robust cyberspace intelligence section and have close ties to the national intelligence community. The JRCC and all the JRCBs need to establish a strong relationship with the Space domain community. All command and critical staff positions should be equitably rotated among the Service's Reserve Components with a percentage set aside for Active Duty and National Guard personnel according to representation. These billets should provide for upward career mobility for officers, warrant officers, and NCOs. Developing and maintaining a core of career personnel staffing for these units is critical – most personnel need to rotate back to their respective Service component in order to spread the benefits of their training and experience. But a select group should commit most of their career to the JRCC (and not be penalized by their respective Service component). All Service Components need to be represented (to include Marine Corps and Coast Guard reserves).

While the composition of many of these units are currently established (IO, signal/comms, electronic warfare, power generation, and intelligence), in some Services the network defense and cyberspace operations battalions need to be developed. Each of the full-spectrum computer network operations (CNO) cyberspace operations battalions should have a roughly equal billet and personnel mix of the following communities: cyberspace operations (for Services with that career field), military intelligence, signals/communications, electronic warfare, information operations, and branch immaterial (cyberspace experts, often with CAS regardless of branch, community, or MOS). The last category is crucial to recruiting and retaining RC personnel with civilian acquired skills whose MOS does not fall into the specified communities. Network defense battalions (cyberspace domain defense missions only) would generally comprise Blue Teams, Red Teams, cyberspace operations assistance teams, a Regional Computer Emergency Response Team (RCERT), and mobile Computer Emergency Response Teams (MCERTs) to support joint task forces and foreign/domestic contingency operations.

Some of these brigades, battalions, and company/detachments could concentrate on sector communities that are either national in nature or prevalent in their geographic area, such as: government, finance & economics, energy, water & utilities, transportation & logistics, communications (satellite, telcos, ISPs), health & insurance, R&D, and manufacturing & technology. Possible other communities (depending upon location and mission) might include agriculture and port & maritime operations. An optional construct for a Functional Joint Cyberspace BDE is also outlined in Figure 2 for illustrative purposes. This brigade would allocate its resources for employment within specific critical communities at the national or regional level rather than have assigned geographic responsibilities. The JRCC staff would adjudicate Lanes in the Road between the JRCBs to ensure that resources are not duplicated or missions fall thru the seams between units. An example could be the establishment of a JCRB that focuses entirely on cyberspace security of the national power grid infrastructure. Another example of the employment of a sub-JCRB unit might be the Area II JCRB commanding a cyberspace operations battalion deployed in New York with an assigned area of responsibility (AOR) for the financial community. It would specialize in working with the financial community, either in Area II or possibly with the financial community nation-wide. Or in another example, companies/flight-level units, platoons, and detachments specializing in network defense supporting port and maritime operations could be established in major sea-going port cities.

The JRCC needs to have the flexibility to adapt to rapidly changing threat, customer, and technology environments. It needs to be able to conduct cyberspace operations regardless of shortfalls in the power and spectrum situation. It must have the agility to reprioritize and reorganize ‗on the move' at Internet speed. This requires the removal or mitigation of the deadening bureaucratic industrial-age rules cultivated over many decades by DoD and the Services (often imposed by Congress). The military Personnel, Acquisition, Mobilization, and Force Management communities & processes provide excellent examples of bureaucratic industrial-age systems that are woefully inadequate in the information-age.

Advantages of this Initiative

DoD has historically been inefficient in its leveraging of civilian acquired skills of its RC personnel. This initiative would allow DoD to catalog those currently hidden skill sets and consolidate, organize, and concentrate employment of cyberspace personnel. It would provide information as to their level of training, identify gaps, and concentrate resources on those gaps. It would provide a much strengthened C2 of a currently fragmented but extremely valuable resource. It represents a highly cost effective solution to a complex problem. Use of DoD's Reserve Components is an extremely cost-effective option in general - DoD's Reserve Components represent 43% of DoD capability but represent 9% of its budget.[8] This proposed

[8] Office of the Assistant Secretary of Defense for Reserve Affairs.

concept ensures that active component personnel and forces can concentrate on military cyberspace operations for US and coalition forces in the event of a large scale national or regional cyberspace incident or major cyberspace warfare. These RC cyberspace units would be available for mobilization in support of military operations in cyberspace and/or to deploy to Combatant Commands to provide forces in support of warfighting requirements. These brigades, battalions, companies, and detachments need to be fully capable of mobilization and overseas deployment into theaters and areas of hostilities (AOH). JCRBs need to be prepared to cover an adjacent Region if the assigned Brigade is mobilized and deployed.

These regional RC brigade commands (JRCBs) would have the advantage of physical proximity to their supported mission. This provides familiarity with the cyberspace terrain, ‗customers' (state/local governments & critical businesses and infrastructure), and allows various Blue Team and other assistance mission units to efficiently travel to local network enclaves to more easily provide on-site support vice a centralized national approach. The JCRBs should establish regional CERTs to support their assigned Federal Region. The JCRBs provide a focal point for state/local governments and businesses to turn to for assistance during a cyberspace event. The Regional commands can send assistance teams on-site to provide support in a rapid and efficient fashion. This construct also provides strong continuity of operations for regional events that adversely affect one JRCB that can be mitigated and addressed by adjacent and surrounding JRCBs.

The Regional Commands need to be closely integrated with DHS and FEMA organizations. It should be clear that these are military units, under military command, organized and resourced by military channels, under UCMJ, etc… They do not come under DHS or FEMA command, supervision, or jurisdiction. However, they can play a support role under circumstances as defined by the National Command Authority. The JRCC and Regional JCRBs J5 sections also need to establish liaisons with private hacker groups such as the Shadowserver Foundation and Hackers for Charity. There are many private non-governmental cyberspace organizations (many of them informal) that engage in charity work, support civil liberties and privacy rights, or exist to fight crime in cyberspace. These organizations have the untapped potential to support many goals in common with the JRCC and JRCBs. Some of these organizations and US citizens perceive a conflict between the military institution and civil liberties/privacy rights. But the US military is sworn to protect the Constitution, and civil liberties and privacy rights are an inherent and crucial part of the Constitution. Citizen-Soldiers constitute one of the best bulwarks for protection of these rights.

These geographically dispersed cyberspace operations units provide considerable assets for continuity of operations and disaster recovery (COOP/DR) planning. These capabilities would support USCYBERCOM and DoD, as well as for the nation as a whole. The JRCC HQ itself could act as one of the COOP/DR site for USCYBERCOM. The JRCC's capability distribution is both geographic and personnel in nature – the regional brigade commands are designed to be diverse in location, focus, expertise, and assembled personnel. At the same time, they must be required to meet stringent standards for personnel, training and operational capabilities. These commands could provide considerable communications and power generation assets and support during natural or man-made disasters. This also allows these commands to align with and act as ‗supporting' commands to USNORTHCOM and DHS under circumstances when they are established as the ‗supported' commands. Cyberspace domain operations typically lend themselves to world-wide strategic events where USCYBERCOM is the ‗supported' command. But there may be circumstances where USCYBERCOM is not the ‗supported' command but is in a position to provide support to other commands, such as DHS/NORTHCOM or other COCOMs. Examples include situations such as a Katrina-type natural disaster (domestic, overseas, or international) or a localized multi-state outage of Internet, electronic telecommunications, and power infrastructure.

This initiative would increase DoD's already maturing partnership with the private sector and continue its long-standing partnerships with state/local governments. It would directly support DoD's mission readiness/capability as DoD is already dependent upon national critical infrastructure to conduct its warfighting missions. For example, DoD is dependent upon civilian infrastructure in the areas of power, utilities, communications, and logistics (supply, acquisition, transportation, etc…) for combat power projection and to accomplish its mission. In turn, these infrastructures are heavily dependent upon their cyberspace infrastructure (computers, databases, Internet, satellites, GPS, RFID, telecommunications, etc…). This initiative would help these critical national infrastructures continue their support to the nation and to DoD's warfighting mission while under attack, compromise, or in the event of a major disaster.

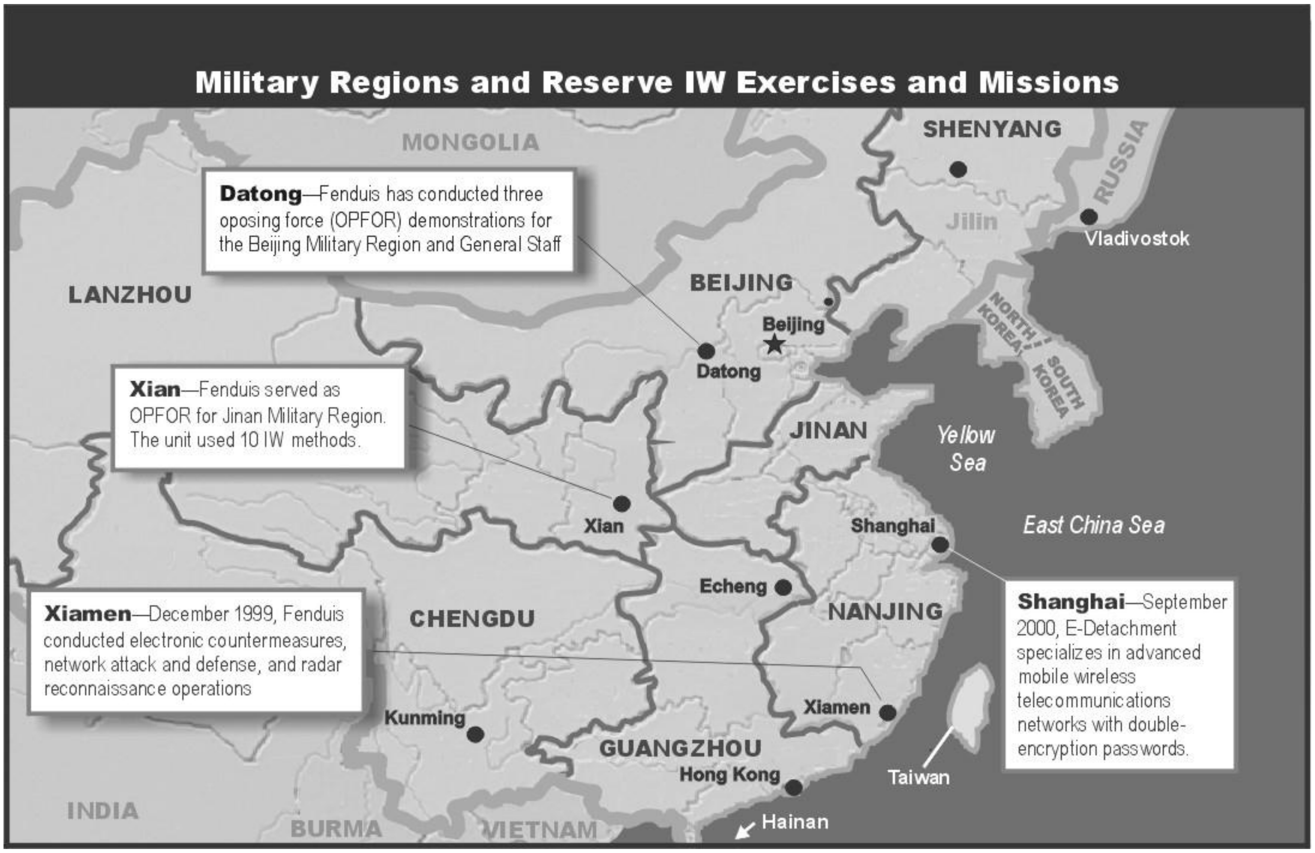
Establishment of the JRCC will provide organization, mission, and billets for former Active Component (AC) military personnel who, after building expensive skill sets at the taxpayer's expense, can be retained in the RC where they are available for recall upon an emergency or contingency. This initiative will help retain these personnel with critical skill sets in the military inventory for several reasons. This initiative allows them to continue their military obligation using skill sets expensively developed (in many cases) at taxpayer expense. It allows them to live close to their homes and employment while still contributing to the nation's defense. In this way they can contribute to the well-being of their local community as well as to the Nation. It also provides an opportunity to retain service-related disabled veterans in military service. These Service Members who are wounded/injured in overseas operations should be double and triple slotted against JRCC billets and receive a waiver for relaxed physical fitness standards. These disabled service members not physically fit for combat or overseas deployment should be retained in a non-deployable status. They would be overstrength to the warfighting requirement but would remain in support of the regional cyberspace requirement regardless of the unit's mobilization and deployment status. Those that are not already trained in cyberspace operations could be provided the necessary training that will not only extend their military service for homeland defense but also provide them with job training that is highly desirable in the private sector, thus helping to reduce veteran unemployment.

This initiative forces DoD to catalog and understand its true RC capability in the cyberspace domain. Once DoD has intellectually captured and understands its full capability, it can organize and align It to meet cyberspace domain threats/requirements. It allows DoD to provide focused individual and collective training to its RC cyberspace elements. These are much needed but sorely lacking improvements that would make a world of difference in a major cyberspace event.

Summary

Only the US Defense Department has both a detailed understanding of the threats and the capacity necessary to deliver significant enhancements to the security of the nation's critical cyber infrastructure in relatively short order. DoD is also the only USG organization with a substantial Reserve Component contingency expansion potential with thousands of highly-capable cyberspace trained personnel that can be mobilized and focused on cyberspace domain threats. This capacity needs to be organized and focused with a robust C2 architecture to achieve its highest potential. There are huge legal, bureaucratic, and resource obstacles that would impede this or a similar plan. The intent of this article is not to minimize the potential obstacles to implementation of this proposed organization – they are quite daunting. But planning and implementing the proposed (or similar) organization needs to take place prior to any cyberspace domain event or major cyberwar – the nature of cyberspace is instantaneous and simultaneous. A threat can hit a totality of targets at the same time and in an instant. If cyberspace organizations and capabilities are not developed prior to an event, it could be over before anything can be lashed together.

This plan represents the Citizen-Soldier concepts of national defense, regional security, and an operational reserve at their finest. Cyberspace is becoming the economic and cultural backbone of the United States and vulnerabilities to cyberspace operations threaten national security. These capabilities outlined in this article need to be organized and focused by USCYBERCOM for the protection of the national security of the United States.



Military Regions and Reserve IW Exercises and Missions

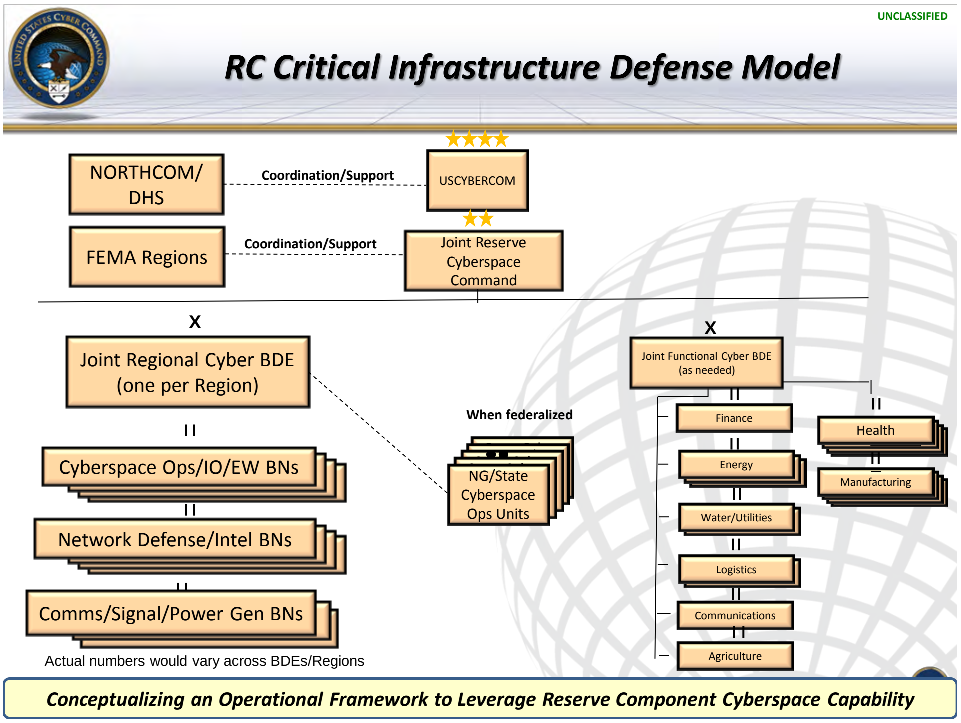
Datong—Fenduis has conducted three oposing force (OPFOR) demonstrations for the Beijing Military Region and General Staff

Xian—Fenduis served as OPFOR for Jinan Military Region. The unit used 10 IW methods.

Xiamen—December 1999, Fenduis conducted electronic countermeasures, network attack and defense, and radar reconnaissance operations

Shanghai—September 2000, E-Detachment specializes in advanced mobile wireless telecommunications networks with double-encryption passwords.

Figure 1:Missions of Cyber Divisions (Fenduis) (From LTC Timothy Thomas, ―China‘s Electronic Strategies" Military Review, 2001)[9]



UNCLASSIFIED

RC Critical Infrastructure Defense Model

NORTHCOM/ DHS

Coordination/Support

USCYBERCOM

FEMA Regions

Coordination/Support

Joint Reserve Cyberspace Command

X

Joint Regional Cyber BDE (one per Region)

II

Cyberspace Ops/IO/EW BNs

II

Network Defense/Intel BNs

II

Comms/Signal/Power Gen BNs

Actual numbers would vary across BDEs/Regions

When federalized

NG/State Cyberspace Ops Units

X

Joint Functional Cyber BDE (as needed)

II

Finance

II

Energy

II

Water/Utilities

II

Logistics

II

Communications

II

Agriculture

II

Health

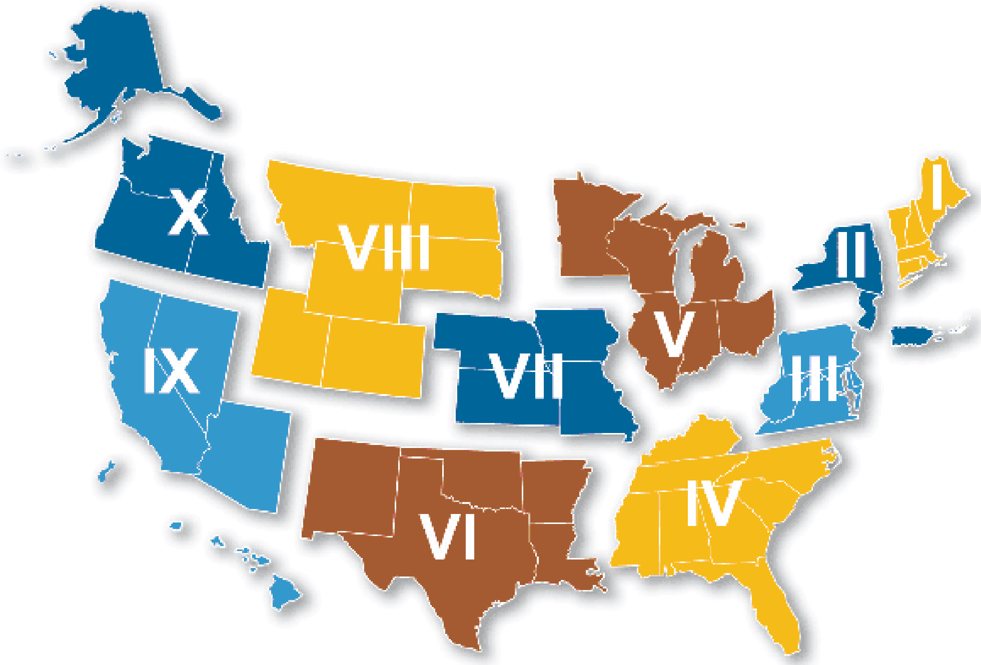
II

Manufacturing

Conceptualizing an Operational Framework to Leverage Reserve Component Cyberspace Capability

Figure 2: Reserve Critical Infrastructure Defense Model

[9] Thomas, Timothy L. —China‘s Electronic Strategies," *Military Review,* May-June 2001. Found at: http://www.au.af.mil/au/awc/awcgate/milreview/thomas.htm —The article noted that in 1991 Chairman Jiang Zemin called for building common telecom systems for military and civilian use to meet peacetime and wartime needs. Only in such fashion could military telecom catch up with its civilian counterpart. One way to do this was to create reserve forces (a key component uniting civilian and military sectors in a people's war) with telecom and IW/IO missions. The paper noted, "We have built a reserve telecom force structure with a reserve telecom regiment as the backbone, with an information industrial department as the base . . . have built a reserve contingent of qualified high-tech telecom and transmission personnel with those specializing in satellite telecom, relay telecom, digital telecom, telegraph (telephone) telecom, and optical-fiber telecom as the main force . . . and have built a contingent of highly qualified personnel with computer experts, network monitoring experts, as well as radio telecom units serving as the backbone." China's reserve forces are now being armed with IW/IO missions and have become the high-tech link in the country's people's war theory. In the past, reserve forces' planned role in a people's war was supporting PLA forces defending against foreign intervention. Today's reserve forces can do something even the PLA could not for many years—reach out and touch someone continents away with electronic and information weapons. Properly targeted electronic attacks could be as devastating to a country's economy as damage inflicted by an intercontinental missile….The reserve forces also reportedly have their own websites and simulation centers."



<u>**Figure 3 – FEMA Regions (from FEMA web site)**</u>

David M. Hollis is a GG-15 Senior Policy Analyst/Planner with the Office of the Undersecretary of Defense for Intelligence's (USD(I)) Cyberspace, Warfighter Integration, and Strategic Engagement Division (CWISE). Prior to this position, he was the Chief of the Cyberspace Security Division for the Office of the Assistant Secretary of Defense for Network & Information Integration /DoD Chief Information Officer (ASD NII/DoD CIO). Lieutenant Colonel David M. Hollis, (USAR, MI) is also currently serving as the Senior USAR officer & USAR Element OIC for the Joint USCYBERCOM. He was previously a drilling Joint Plans Officer with the USSTRATCOM Joint Functional Component Command for Network Warfare (JFCC-NW) J5. Prior to his current USAR assignment, LTC Hollis was assigned/mobilized with the Army 1st Information Operations Command as Senior Operations Planner, S2/Chief of the Army CyberIntelligence Center, and Army Red Team Chief. Prior to 1st IOC, he was the Senior VP at Cryptek Secure Communications and Director of Federal Operations at Secure Computing Corporation. His background encompasses almost 30 years of government, military and private sector/commercial cyberspace experience starting in 1982 as a GS-4 communications engineering technician with the Naval Electronic Systems Command. He was commissioned through ROTC at Old Dominion University in 1985 with an undergraduate degree in engineering and earned an MBA from Strayer University in 1998. He is a graduate of the Army's Command and General Staff College and the Joint Forces Staff College's Advanced Joint Professional Military Education. He has previously written four articles on cyberspace domain operations for Joint Forces Quarterly, Armed Forces Journal, and Small Wars Journal; and one article for a Civil War magazine/blog on the strategic effect of railroads during the Civil War.